GUIDELINES FOR WASHINGTON STATE LAW ENFORCEMENT

Operation of Automated License Plate Readers

WASHINGTON ASSOCIATION OF SHERIFFS AND POLICE CHIEFS

September 2008

TABLE OF CONTENTS

PURPOSE OF GUIDELINES

The Automated License Plate Reader Guidelines are non-binding guidelines, voluntarily adopted by the Washington Association of Sheriffs and Police Chiefs as means of improving the operation and management of Automated License Plate Reader equipment and data and facilitating compliance with all applicable laws.

The Guidelines will be most effective if used as the minimum framework in the development of local policies regarding the use of Automated License Plate Readers.

The Guidelines are based on legal requirements and the application of the experience of jurisdictions that have used Automated License Plate Readers. They are not intended as a substitute for professional judgment and common sense nor are they intended as legal authority or as legal advice. Counties, cities and agencies should involve their individual legal counsels in determining the answers to legal questions related to policy, procedure, and practice.

I. BACKGROUND

A model policy on the use of Automated License Plate Readers is needed to provide guidance to agencies in the use of the new technology. While ALPRs enhance public safety by increasing law enforcement efficiency, public concerns regarding privacy implications of the technology should be addressed.

ALPRs assist Washington law enforcement in the ongoing efforts to reduce the problem of auto theft.[1]

- In Washington, on average, a car is stolen every 14 minutes and 100 cars are stolen every day. Washington ranks fifth in the nation for stolen vehicles. Nearly 45,000 vehicles were stolen in Washington in 2006 and 36,439 vehicles were stolen in 2007 (-19%).[2] In 2005, auto thefts cost Washington citizens over $325 million in higher insurance rates and lost vehicles.
- Auto theft is linked to other crimes, as offenders use stolen vehicles for robbery, burglary, assault, and drugs. Many people stopped in stolen vehicles possess misappropriated personal identification, drugs including methamphetamine and its precursors, and drug manufacturing equipment.
- ALPR technology is a part of larger efforts to combat auto theft and related crimes and will lead to quicker recovery and return of stolen vehicles. In fact, Washington is already #1 nationally for stolen vehicle recovery (91% recovered in 2007). This translates into millions of dollars in potential savings to victims and their insurers.

The concept of using cameras as a method to record a vehicle passing a specific location and then identifying the owner or operator began in the 1970's. Use of prior technology

[1] Washington Auto Theft Prevention Authority PowerPoint, April 3, 2008.
[2] Theft statistics obtained from Crime in Washington , 2007 (UCR data prepared by WASPC)

has proved to be time consuming, particularly for the officer entering information. It is also expensive to operate, and capture, convert and store information and is limited by lighting and weather conditions.[3]

Several law enforcement jurisdictions have been using ALPR technology prior to 2008. In addition, the Washington Auto Theft Prevention Authority, in mid-2008, allocated funding for local jurisdictions' acquisition of ALPRs in 2008.[4] This funding was conditioned on adoption of guidelines for the usage of ALPRs. Other current activities include the Washington State Patrol use of ALPRs to screen vehicles boarding ferries and the Seattle Police Department's ongoing efforts to combat the approximately 9,000 stolen vehicles a year.[5]

ALPR technology will be useful for law enforcement in a variety of ways, including AMBER alerts and missing persons and tracking down those with outstanding warrants. Jurisdictions around the country have used the technology for a wide-range of activities including placing a suspect at a scene of a crime, terror watch list hits, identifying witnesses, combating organized crime and gangs, and tracking registered sex offenders or those under supervision.

AUTOMATED LICENSE PLATE READER TECHNOLOGY[6]

Automated License Plate Reader Technology (ALPR), also known as License Plate Recognition, provides automated detection of license plates. Its primary function is to convert data taken in the field from vehicle plates and use it for the law enforcement purposes of identifying stolen vehicles, stolen license plates, and missing persons. ALPRs are also used to gather information related to active warrants, homeland security, electronic surveillance, suspect interdiction and stolen property recovery. ALPR data can be stored for later use.

An ALPR system is a computerized system consisting of specialized digital cameras, a processor unit and a laptop computer. The mobile camera system mounted on police patrol vehicles recognizes plates in real time. ALPR systems can identify a target plate within seconds of contact with it. An ALPR can recognize over 1,000 license plates an

---

[3] Transportation Research Board, 2002. "Effects of Ambient Light, Camcorders, and Automated License Plate Reader Settings on Plate Transcription Rates," cited in *Operation of License Plate Readers For Law Enforcement Agencies In New York State* Suggested Guidelines, June 2008, New York, Division of Criminal Justice Services

[4] Washington Auto Theft Prevention Authority (RCW 46.66.010) receives funding from an account created in the Washington State Treasury. The Authority allocates moneys appropriated from the account to public agencies for the purpose of establishing, maintaining, and supporting programs designed to prevent motor vehicle theft, including financial support for the procurement of equipment and technologies for use by law enforcement, such as ALPRs.

[5] http://www.seattle.gov/police/programs/technology/license_plate_reader.htm

[6] Information in this subsection and throughout this document has been taken in part, and occasionally verbatim, from *Operation of License Plate Readers for Law Enforcement Agencies in New York State* Suggested Guidelines, June 2008, New York, Division of Criminal Justice Services.

hour on vehicles as they pass either a portable or stationary unit. A range of camera systems are available, most capable of reading license plates day and night and in a variety of weather conditions. ALPR systems typically include infrared strobe and camera systems that can take high speed, high contrast images read at closing speeds of 150 miles per hour.

An ALPR reads a plate and compares it against a database of suspect vehicles, alerting the officer to any matches. It uses a large list of target plates stored locally in a "hot list" rather than relying on real-time communications with State or Federal data sources. The list is typically transferred daily and can be updated by the operator or by a central station if wireless communications are not available in the vehicle. The hot list can contain any set of plate data, including watch lists as well as stolen vehicles. When a target plate is located, the officer in the vehicle is notified with a message that is specific to the plate. This hit occurs even if the driver of the vehicle has not committed a traffic offense or been involved in a traffic accident.

DATABASES

In Washington, the information downloaded will come from the NCIC hot file via ACCESS (A Central Computerized Enforcement Service System), currently managed by the Washington State Patrol (WSP). NCIC contains national stolen vehicle and plate data published daily by the FBI. The WSP places the NCIC file on a server available through ACCESS to those agencies that have a specific and signed agreement with WSP to access and use the information. There may be other files local law enforcement may use if a local jurisdiction wishes to up load them. This could include access to a local record management system, parking violations, or warrant data.

Lists can be updated manually if the officer enters a specific plate into the system and wants to be alerted when the plate is located. The system can also alert the officer if the new addition was recently seen. Integrated GPS technology allows the operator to locate the last contact with the vehicle.

ALPR systems also record every license plate they view. Some systems record the location, date and time of each license plate read. This intelligence resource is available as a law enforcement tool, allowing the officer to identify the last known contact with a vehicle and also to report the list of vehicles located in a specific area at a given time range.

HARDWARE

Most ALPR systems include a set of cameras that have infrared illumination capabilities. "Progressive" cameras capture images in various lighting conditions by actively managing infrared strobes integrated into the cameras. These cameras are mounted outside of the vehicle as auto glass can interfere with their operation. The cameras are mounted either permanently on the rooftop, magnetically in a transportable configuration, integrated into the light bar on a marked vehicle, or within a covert housing.
The two types of units are:

1. Portable unit - can be moved from vehicle to vehicle.
2. Fixed unit - hard mounted to a marked patrol vehicle or in a fixed location.

Cameras connect to a computer and a display. ALPR systems typically only require the operator to have one computer display in the vehicle. The processor in an ALPR system can include a specialized computer that manages the cameras and allows the system to run at very high speeds regardless of the speed or power of the existing in-car PC/Laptop.

SOFTWARE

ALPR software typically has three components: character translation; hot list management and user interface. The user interface manages the activity and allows the officer to identify an alarm and the target vehicle. In most cases, most of the screen space on the user interface is reserved for the target vehicle/plate photo as that is the primary means for alarm vehicle identification.

The interface also allows the user to enter additional target plates, check on the information in the hot list and respond to visual and audible alarm queues.

II. SUGGESTED GUIDELINES FOR PATROL AND INVESTIGATIONS

The following guidelines are the suggested protocols for using ALPRs and their attendant databases and information. Use of ALPRs should be restricted to the purposes outlined in these guidelines. No officer should use, or authorize the use of, the equipment or database records for any non-approved reason.

ADMINISTRATION

The agency shall designate a system administrator, consistent with WACIC guidelines, who is responsible for the following:

- Overseeing and administering the ALPR program, including the storage and management of all ALPR data systems.
- Ensuring the proper selection of the personnel approved to operate the ALPR system.
- Ensuring appropriate training of operators and that training is completed prior to an operator using the system.
- Ensuring that all training is documented.
- Ensuring the provision of ongoing training as deemed necessary.
- Authorizing any requests for ALPR use or data access according to the guidelines.

ALPR OPERATOR SELECTION

Any agency personnel permitted to access historical ALPR data must meet the same criteria as other agency employees, including law enforcement, regarding authorization

to access to data. This includes but is not limited to polygraphs, fingerprints and background checks.

TRAINING

- An Operator is prohibited from using the ALPR system until properly trained in its use, and after he or she has been instructed as to operational protocols.
- Operators must be ACCESS certified prior to accessing ALPR data.

ALPR USAGE

- ALPR operation and access to ALPR collected data shall be for official agency purposes only.
- ALPRs may be used during any routine patrol or criminal investigation. Reasonable suspicion or probable cause is not necessary (see III. Legal Issues below).
- ALPR equipped cars should be made available to conduct license plate canvasses for all homicides, shootings and other major crimes or incidents. ALPR may be used to conduct grid searches of all blocks around the crime scene. Partial plates reported during major crimes should be entered into the ALPR in an attempt to identify suspected perpetrator's vehicles.
- Each agency using ALPRs shall have a policy regarding recovery of stolen vehicles.
- The agency shall document and maintain records of all ALPR operators and their ALPR usage.

DATA COLLECTION AND RETENTION

- All ALPR data recorded should be maintained on the operator's laptop for a maximum of 24 hours from the end of the officer's shift during which the data was recorded.
- All ALPR data recorded during a shift should be downloaded within 24 hours to an authorized server. Once the data is transferred it shall be purged immediately, or as soon as practicable, from the ALPR/laptop.
- All ALPR data downloaded to the operator lap top and server must be accessible only through a login/password accessible system capable of documenting who accesses the information by identity, date and time.
- Only those with ACCESS Level I certification may access ALPR data. All requests for access to stored ALPR data must be logged, and a stated purpose for access must be provided.
- Requests to review stored data shall be recorded and maintained in the same manner as criminal history logs.
- All ALPR data downloaded to the server may be stored for a period up to but no longer than 60 days prior to purging. Data must be purged once the maximum retention period has been reached unless it has become or it is reasonable to believe it will become evidence in a specific criminal or civil action. In those

circumstances, the applicable data shall be downloaded from the server onto a CD or other portable technology. It shall be subject to the same logging, handling and chain of custody requirements as other evidence.

- Persons approved to access ALPR data under these guidelines are permitted to access the data when there is an articulable suspicion that the data relates to an investigation in a specific criminal or civil action
- Notwithstanding any other provision of law, all electronic images or data gathered by Automated License Plate Readers are for the exclusive use of law enforcement in the discharge of duties and are not to be made open to the public. However, nothing in these guidelines should be interpreted to limit the use of the electronic images or data for legitimate purposes by prosecutors or others legally permitted to receive evidence under the law.

III. LEGAL CONSIDERATIONS

A. CONSTITUTIONAL IMPLICATIONS

The following legal analysis concerning the use of automated license plate readers is advisory only and is meant to provide guidance to agencies in developing a policy to govern the use of ALPRs. It is strongly recommended that each law enforcement agency consult with its own legal advisor prior to adopting a policy regarding the use of ALPRs.

Prior to expanding the use of ALPRs it is important to review whether law enforcement use of the technology implicates the privacy protections of either the 4th Amendment of the Federal Constitution or Article 1, Section 7 of the Washington State Constitution[7], and whether it is likely that a court would place restrictions on law enforcement's use of ALPRs.

It has been well-settled by courts, including those in the 9th Circuit and Washington State, that a law enforcement officer's database search of a specific license plate number obtained from a vehicle in public view does not implicate, and thus cannot violate, an owner's or driver's constitutionally protected expectation of privacy under either the state or federal constitutions. The Washington courts have not found that a reasonable expectation of privacy exists in one's license plate number or in the information attached to it in remote databases. Therefore, law enforcement license plate searches revealing information about a person's car ownership, driver status and criminal record are not searches and do not trigger constitutional protections. See United States v. Diaz-Castaneda, 494 F.3d 1146 (9th Cir. 2007); State v. McKinney, 148 Wn.2d 20, 60 P.3d 46 (2002); State v McCue, 2003 Wash. App. LEXIS 2788 (Wash. Ct. App.); State v. Martin, 106 Wn.App.850 (2001); Seattle v. Yeager, 67 Wn. App. 41, 834 P.2d 73 (1992); United States v. Grigg, 498 F.3d 1070, 1082, 2007 U.S. App. LEXIS 19922 (9th Cir. Idaho 2007); United States v. Neal, 2007 U.S. Dist. LEXIS 89696 (D. Or. Dec. 3, 2007).

[7]Article 1, Section 7 reads: "Invasion of Private Affairs or Home Prohibited: No person shall be disturbed in his private affairs, or his home invaded, without authority of law." The Fourth Amendment to the United States Constitution provides the "right of the people to be secure in their persons, houses, papers, and effects, against unreasonable searches and seizures." U.S. Const. amend. IV; Mapp v. Ohio, 367 U.S. 643, 81 S. Ct. 1684, 6 L. Ed. 2d 1081 (1961).

As a result, law enforcement is not required to meet well established constitutional standards regarding searches or seizures in order to properly enter a license plate into a database or conduct a computerized search.[8] Because a license plate reader merely accomplishes, more efficiently, the same task that a police officer may accomplish by reading a license plate and manually entering the number into a database, it is reasonable to assume that a court would not hold that using an ALPR constitutes a search.

The use of license plate database searches and ALPRs can be contrasted with the impermissible warrantless, random searches of names entered into a motel register,[9] law enforcement access to telephone records,[10] or law enforcement use of thermal imaging devices to monitor heat patterns inside private residences.[11] A license plate is by nature voluntarily placed in a public location with the expectation that it will potentially be viewed by any member of the public, including a law enforcement officer. Motor vehicle records are kept by the state primarily for state use and drivers and owners are presumed to know that the records are available to the police as well. State v. Harlow, 85 Wn. App. 557 (1997).

It appears that every other jurisdiction that has addressed this issue has reached the same conclusion as Washington courts. For example, the Tenth Circuit has held on at least two occasions that license plates are "in plain view on the outside of the car" and thus, are "subject to seizure" because there is no reasonable expectation of privacy. United States v. Matthews, 615 F.2d 1279, 1285 (10th Cir. 1980). See also United States v. Walraven, 892 F.2d 972, 974 (10th Cir. 1989); United States v. Crooks, 2008 U.S. Dist. LEXIS 35189 (D. Del. Apr. 29, 2008); United States v. Ellison, 462 F.3d 557, 561-563 (6th Cir. 2007).

However, it should be noted that the ALPR technology is relatively new and its capabilities are expanding rapidly. As yet, no appellate or higher court in the country has specifically reached a decision based on a challenge to the use of the ALPRs and their ability to facilitate the random scanning of multiple vehicles in a given location over a given time period. Nor have cases specifically addressed the use of ALPRs to search databases beyond typical DOL databases or criminal databases containing warrant information. They have also not addressed the storing of information from ALPRs.

---

[8] See e.g. Katz v. United States, 389 U.S. 347, 357, 88 S. Ct. 507, 19 L. Ed. 2d 576 (1967) for an outline of 4th amendment constitutional standards regarding searches and seizures.

[9] See *State v. Jorden*, 160 Wn.2d 121, 156 P.3d 893 (2007). Court noted that register reveals sensitive information including one's whereabouts in a motel and one's associates.

[10] See Gunwall, 106 Wn.2d 54 (1986). The court held that the police violated privacy rights by obtaining phone records without a warrant and using a monitoring device to record the numbers dialed on the telephone.

[11] State v. Young, 123 Wn.2d 173, 867 P.2d 593 (1994). Warrant needed for use of thermal imaging devices to monitor heat patterns inside private residences because such surveillance "discloses information about activities occurring within the confines of the home, and which a person is entitled to keep from disclosure absent a warrant."

Based on discussions in various court opinions, it is possible that courts might look less favorably on extensive gathering and retention of information beyond that directly associated with a license plate or criminal database, or the gathering of information which a citizen would reasonably expect would be private. This may include the random use of an ALPR to capture information that might be used to create inferences about a vehicle owner's associates or about his activities in his home.

Given the legal reasoning of the courts, ALPR model policy guidelines should consider what databases will be accessed for use with an ALPR, and how long information will be stored both in the vehicle and on a remote server. It should also address what parameters will be used regarding the use of ALPR information to track the movements and location of vehicles on a given date or time. Specific policies and procedures should also address prevention of potential abuse of the technology and outline the necessary safeguards.

B. BRADY AND REQUIRED DISCLOSURE OF EVIDENCE

Information obtained from use of ALPRs may be subject to the rules of both Brady and Washington's rules of discovery.

Brady v. Maryland held that "suppression by the prosecution of evidence favorable to an accused violates due process where the evidence is material to either guilt or to punishment, irrespective of the good faith or bad faith of the prosecution." Brady v. Maryland, 373 U.S. 83, 83 S. Ct. 1194, 10 L. Ed. 2d 215 (1963); Strikler v. Green, 527 US 263 (1999). The rule applies to exculpatory and impeachment evidence likely to change the result in the defendant's favor on an issue of guilt or eventual punishment if convicted. This test applies to matters arising before, during or after trial and applies whether the defense has requested the information or not.

A defendant is within his rights to request a prosecuting attorney attempt to make information available that may be in the control of or known only to others. Kyles v. Whitley, 514 U.S. 419 (1995). The individual prosecutor has a duty to learn of any favorable evidence known to the others acting on the government's behalf in this case, including law enforcement. Id. The good faith or bad faith actions of state actors are irrelevant when the state fails to disclose material exculpatory evidence to the defense under Brady, but where potentially useful evidence is concerned, only bad faith actions on the part of state actors will be said to violate a defendant's rights. See State v. Copeland, 130 Wn.2d 244; Arizona v. Youngblood, 488 U.S. 51, 58, 102 L. Ed. 2d 281, 109 S. Ct. 333 (1988).

Violations of Brady are usually grounds for a new trial, but they can also support a motion to dismiss a prosecution altogether. United States v. Chapman, No. 06-10316 (9th Cir. 2008). Therefore it is best practice for both prosecutors and law enforcement to resolve Brady questions in favor of disclosure.

In addition to constitutional due process protections governing the Brady rules, Washington has reciprocal discovery rules in criminal matters which obligate prosecutors and law enforcement. See CrR 4.7 and CrRLJ 4.7. These rules govern

disclosure of inculpatory and exculpatory evidence. However, in contrast to Brady, the prosecutor is only obligated to turn over information and materials that are in his or her possession or control. One must go beyond these discovery rules to comport with the constitutional rules of Brady, as described above.

Because ALPR information may be used as evidence in future proceedings and subject to Brady, agencies should follow existing Brady protocols when in receipt of ALPR evidence that could be Brady material.[12] However, it does not appear that law enforcement is required to store ALPR information for any specific length of time simply because it might potentially be Brady evidence at some unknown point in the future.

If an agency does not have Brady protocols, it is recommended the agency draft such protocols, and include provisions regarding ALPRs. It may be useful for any database maintaining the ALPR information to have the capability to categorize data as potential or actual Brady material.

[12] One example addressing license plate information as Brady evidence is the U.S. Supreme Court's decision in Kyles v. Whitley, 514 U.S. 419, 438 (1995). There, the Court found law enforcement crime scene notations regarding license plates to be Brady material. Specifically, the prosecution's list of cars at a crime scene after a murder were to have had some value as exculpatory evidence when the license plate of the defendant was not included on that list. It was considered impeachment of the prosecution's arguments to the jury that the defendant had left his car at the scene during the time in question.